

第 2-1 表 原子炉設置変更許可申請書と設計及び工事の計画との整合性

設置変更許可申請書（本文）	設置変更許可申請書（添付書類八）該当事項	設計及び工事の計画 該当事項	整合性	備考
<p>五 発電用原子炉及びその附属施設の位置、構造及び設備</p> <p>ロ 発電用原子炉施設の一般構造</p> <p>(3) その他の主要な構造</p> <p>(i) 本発電用原子炉施設は、「(1) 耐震構造」, 「(2) 耐津波構造」に加え、以下の基本的方針のもとに安全設計を行う。</p> <p>a. 設計基準対象施設</p> <p>(s) 安全保護回路</p> <p>① <u>安全保護回路を構成するデジタル計算機は、不正アクセス行為に対する安全保護回路の物理的分離及び機能的分離を行うとともに、ソフトウェアは設計、製作、試験及び変更管理の各段階で検証と妥当性の確認を適切に行うことで、不正アクセス行為その他の電子計算機に使用目的に沿うべき動作をさせず、又は使用目的に反する動作をさせる行為による被害を防止することができる設計とする。</u></p>	<p>1. 安全設計</p> <p>1.1 安全設計の方針</p> <p>1.1.5 安全保護回路設計の基本方針</p> <p><u>安全保護系については、不正アクセス行為その他の電子計算機に使用目的に沿うべき動作をさせず、又は使用目的に反する動作をさせる行為による被害を防止する設計とする。</u></p> <p>(安全保護回路)</p> <p>適合のための設計方針</p> <p>六 安全保護系のデジタル計算機は、これが収納された盤の施錠等により、ハードウェアを直接接続させない措置を実施することで物理的に分離し、外部ネットワークへのデータ伝送の必要がある場合は、ゲートウェイを介して一方向通信（送信のみ）に制限することで機能的に分離するとともに、計算機固有のプログラム及び言語の使用による一般的なコンピュータウイルスが動作しない環境などによりウイルス等の侵入防止をすることでソフトウェアの内部管理の強化を図り、外部からの不正アクセスを防止する設計とする。</p> <p>また、「安全保護系へのデジタル計算機の適用に関する規程」(JEAC 4620-2008) 及び「デジタル安全保護系の検証及び妥当性確認に関する指針」(JEAG 4609-2008) に準じて設計、製作、試験及び変更管理の各段階で検証及び妥当性確認（コンピュータウイルスの混入防止含む。）がなされたソフトウェアを使用するとともに、発電所での出入管理による物理的アクセスの制限及び安全保護系のデジタル計算機のパスワード管理による電氣的アクセスの制限により、不正な変更等による承認されていない動作や変更を防止する設計とする。</p>	<p>【計測制御系統施設】（基本設計方針）</p> <p>1.3 安全保護装置等</p> <p>1.3.1 安全保護装置</p> <p>(2) 安全保護装置の不正アクセス行為等の被害の防止</p> <p>① <u>安全保護装置は、外部ネットワークと物理的分離及び機能的分離、外部ネットワークからの遠隔操作の防止、ソフトウェアの内部管理の強化によるウイルス等の侵入の防止、物理的及び電氣的アクセスの制限、システムの据付、更新、試験、保守等で、承認されていない者の操作及びウイルス等の侵入を防止すること等の措置を講じることで①不正アクセス行為その他の電子計算機に使用目的に沿うべき動作をさせず、又は使用目的に反する動作をさせる行為による被害を防止できる設計とする</u>とともに安全保護装置の論理演算機能（作動（起動）回路）については、デジタル回路及びアナログ回路で構成する設計とする。</p> <p>安全保護装置が収納された盤の施錠等により、ハードウェアを直接接続させない措置を実施すること及び① <u>安全保護装置のソフトウェアは設計、製作、試験及び変更管理の各段階で検証と妥当性の確認を適切に行うことで不正アクセスを防止する。</u></p>	<p>設計及び工事の計画の①は、設置許可申請書（本文）の①を具体的に記載しており、整合している。</p>	

第2-1表 原子炉設置変更許可申請書と設計及び工事の計画との整合性

設置変更許可申請書 (本文)	設置変更許可申請書 (添付書類八) 該当事項	設計及び工事の計画 該当事項	整合性	備考																						
			(2/4)																							
	<p>変更前</p> <p>d 安全保護系等の制御方法 (a) 安全保護系の制御方法 イ 原子炉非常停止信号による原子炉非常停止機能 原子炉非常停止信号の作動回路は多重チャンネル構成で“2 out of 4”方式などの論理回路及び原子炉トリップ遮断器^(注2)で構成され、原子炉非常停止を行う。 原子炉非常停止信号の検出部及び論理回路部^(注3)は、検出部又は論理回路部の駆動源喪失等が生じた場合において、原子炉非常停止信号を発信するとともに、警報を中央制御室に表示する。</p> <p>制御方式及び制御方法 発電用原子炉の制御方法</p>	<p>変更後</p> <p>d 安全保護系等の制御方法 (a) 安全保護系の制御方法 イ 原子炉非常停止信号による原子炉非常停止機能 原子炉非常停止信号の作動回路は多重チャンネル構成で“2 out of 4”方式などの論理回路及び原子炉トリップ遮断器で構成され、原子炉非常停止を行う。 原子炉非常停止信号の検出部及び論理回路部^(注3)は、検出部又は論理回路部の駆動源喪失等が生じた場合において、原子炉非常停止信号を発信するとともに、警報を中央制御室に表示する。 原子炉非常停止信号の論理回路は、マイクロプロセッサを用いたデジタル制御装置を適用し、検証及びハードウェアと統合されたシステムに対する妥当性確認を行ったソフトウェアを使用する。</p> <table border="1"> <tr><th colspan="2">原子炉非常停止信号の作動回路</th></tr> <tr><td>種 類</td><td>マイクロプロセッサを用いたデジタル制御装置</td></tr> <tr><td>演算処理方式</td><td>シングルタスク方式</td></tr> <tr><td>デジタル制御装置の個数</td><td>論理回路：4</td></tr> <tr><td>自己診断</td><td>マイクロプロセッサの停止、通信の遮断等を早期に検知し、警報を発信するとともに、保護機能喪失の場合は当該チャンネルをトリップ状態とする</td></tr> <tr><td rowspan="3">環境条件</td><td>温 度</td><td>0～50℃</td></tr> <tr><td>湿 度</td><td>10～95%RH</td></tr> <tr><td>放射線量</td><td>放射線の影響のないこと（非管理区域に設置）</td></tr> <tr><td>応答時間</td><td>秒以下 プロセス信号がデジタル制御装置に入力されてから、原子炉非常停止信号が原子炉トリップ遮断器へ出力されるまで。ただし、チャンネル間データ通信を行わない原子炉非常停止信号は、秒以下</td></tr> <tr><td>データ通信</td><td>計測制御系と電氣的及び機能的に分離</td></tr> <tr><td>外部ネットワークとの遮断</td><td>外部ネットワークへの直接接続なし</td></tr> </table> <p>制御方式及び制御方法 発電用原子炉の制御方法</p>	原子炉非常停止信号の作動回路		種 類	マイクロプロセッサを用いたデジタル制御装置	演算処理方式	シングルタスク方式	デジタル制御装置の個数	論理回路：4	自己診断	マイクロプロセッサの停止、通信の遮断等を早期に検知し、警報を発信するとともに、保護機能喪失の場合は当該チャンネルをトリップ状態とする	環境条件	温 度	0～50℃	湿 度	10～95%RH	放射線量	放射線の影響のないこと（非管理区域に設置）	応答時間	秒以下 プロセス信号がデジタル制御装置に入力されてから、原子炉非常停止信号が原子炉トリップ遮断器へ出力されるまで。ただし、チャンネル間データ通信を行わない原子炉非常停止信号は、秒以下	データ通信	計測制御系と電氣的及び機能的に分離	外部ネットワークとの遮断	外部ネットワークへの直接接続なし	①
原子炉非常停止信号の作動回路																										
種 類	マイクロプロセッサを用いたデジタル制御装置																									
演算処理方式	シングルタスク方式																									
デジタル制御装置の個数	論理回路：4																									
自己診断	マイクロプロセッサの停止、通信の遮断等を早期に検知し、警報を発信するとともに、保護機能喪失の場合は当該チャンネルをトリップ状態とする																									
環境条件	温 度	0～50℃																								
	湿 度	10～95%RH																								
	放射線量	放射線の影響のないこと（非管理区域に設置）																								
応答時間	秒以下 プロセス信号がデジタル制御装置に入力されてから、原子炉非常停止信号が原子炉トリップ遮断器へ出力されるまで。ただし、チャンネル間データ通信を行わない原子炉非常停止信号は、秒以下																									
データ通信	計測制御系と電氣的及び機能的に分離																									
外部ネットワークとの遮断	外部ネットワークへの直接接続なし																									
			(3/4)																							
	<p>変更前</p> <p>ロ 工学的安全施設作動信号による工学的安全施設の作動機能 工学的安全施設作動信号の作動回路は多重チャンネル構成で“2 out of 4”方式などの論理回路及び作動装置で構成され、工学的安全施設を起動させる。 工学的安全施設作動信号の検出部は駆動源の喪失が生じた場合において、フェイル・セーフとなり、工学的安全施設作動信号が発信する。ただし、一部の検出部[*]及び論理回路部は、駆動源の喪失が生じた場合において、工学的安全施設作動信号を作動させず原子炉施設への安全上の支障がない状態を維持する設計(フェイル・アズ・イズ)とし、駆動源が喪失したことを運転員が確実に認知できるよう中央制御室に警報を表示する。なお、単一チャンネルの駆動源が喪失した場合においても、残りのチャンネルによって安全保護系の機能は確保される。 ※原子炉格納容器スプレイ作動信号(原子炉格納容器圧力異常高)を指す。</p> <p>制御方式及び制御方法 発電用原子炉の制御方法</p>	<p>変更後</p> <p>ロ 工学的安全施設作動信号による工学的安全施設の作動機能 工学的安全施設作動信号の作動回路は多重チャンネル構成で“2 out of 4”方式などの論理回路及び作動装置で構成され、工学的安全施設を起動させる。 工学的安全施設作動信号の検出部は駆動源の喪失が生じた場合において、フェイル・セーフとなり、工学的安全施設作動信号が発信する。ただし、一部の検出部[*]及び論理回路部は、駆動源の喪失が生じた場合において、工学的安全施設作動信号を作動させず原子炉施設への安全上の支障がない状態を維持する設計(フェイル・アズ・イズ)とし、駆動源が喪失したことを運転員が確実に認知できるよう中央制御室に警報を表示する。なお、単一チャンネルの駆動源が喪失した場合においても、残りのチャンネルによって安全保護系の機能は確保される。 工学的安全施設作動信号の論理回路は、マイクロプロセッサを用いたデジタル制御装置を適用し、検証及びハードウェアと統合されたシステムに対する妥当性確認を行ったソフトウェアを使用する。 ※原子炉格納容器スプレイ作動信号(原子炉格納容器圧力異常高)を指す。</p> <table border="1"> <tr><th colspan="2">工学的安全施設作動信号の作動回路</th></tr> <tr><td>種 類</td><td>マイクロプロセッサを用いたデジタル制御装置</td></tr> <tr><td>演算処理方式</td><td>シングルタスク方式</td></tr> <tr><td>デジタル制御装置の個数</td><td>論理回路：4</td></tr> <tr><td>自己診断</td><td>マイクロプロセッサの停止、通信の遮断等を早期に検知し、警報を発信するとともに、異常な信号を出力しないようにする</td></tr> <tr><td rowspan="3">環境条件</td><td>温 度</td><td>0～50℃</td></tr> <tr><td>湿 度</td><td>10～95%RH</td></tr> <tr><td>放射線量</td><td>放射線の影響のないこと（非管理区域に設置）</td></tr> <tr><td>応答時間</td><td>秒以下 プロセス信号がデジタル制御装置に入力されてから、工学的安全施設作動信号が出力されるまで</td></tr> <tr><td>データ通信</td><td>計測制御系と電氣的及び機能的に分離</td></tr> <tr><td>外部ネットワークとの遮断</td><td>外部ネットワークへの直接接続なし</td></tr> </table> <p>制御方式及び制御方法 発電用原子炉の制御方法</p>	工学的安全施設作動信号の作動回路		種 類	マイクロプロセッサを用いたデジタル制御装置	演算処理方式	シングルタスク方式	デジタル制御装置の個数	論理回路：4	自己診断	マイクロプロセッサの停止、通信の遮断等を早期に検知し、警報を発信するとともに、異常な信号を出力しないようにする	環境条件	温 度	0～50℃	湿 度	10～95%RH	放射線量	放射線の影響のないこと（非管理区域に設置）	応答時間	秒以下 プロセス信号がデジタル制御装置に入力されてから、工学的安全施設作動信号が出力されるまで	データ通信	計測制御系と電氣的及び機能的に分離	外部ネットワークとの遮断	外部ネットワークへの直接接続なし	①
工学的安全施設作動信号の作動回路																										
種 類	マイクロプロセッサを用いたデジタル制御装置																									
演算処理方式	シングルタスク方式																									
デジタル制御装置の個数	論理回路：4																									
自己診断	マイクロプロセッサの停止、通信の遮断等を早期に検知し、警報を発信するとともに、異常な信号を出力しないようにする																									
環境条件	温 度	0～50℃																								
	湿 度	10～95%RH																								
	放射線量	放射線の影響のないこと（非管理区域に設置）																								
応答時間	秒以下 プロセス信号がデジタル制御装置に入力されてから、工学的安全施設作動信号が出力されるまで																									
データ通信	計測制御系と電氣的及び機能的に分離																									
外部ネットワークとの遮断	外部ネットワークへの直接接続なし																									

本資料のうち、枠囲みの内容は、商業機密あるいは防護上の観点から公開できません。

第2-1表 原子炉設置変更許可申請書と設計及び工事の計画との整合性

設置変更許可申請書（本文）	設置変更許可申請書（添付書類八）該当事項	設計及び工事の計画 該当事項	整合性	備考
<p>五 発電用原子炉及びその附属施設の位置、構造及び設備</p> <p>へ 計測制御系統施設の構造及び設備</p> <p>(2)安全保護回路</p> <p>②安全保護回路は、不正アクセス行為その他の電子計算機に使用目的に沿うべき動作をさせず、又は使用目的に反する動作をさせる行為による被害を防止する設計とする。</p>	<p>6.3.2 設計方針</p> <p>(1) 安全保護系のプロセス計装は、以下の方針で設計する。</p> <p>g. <u>安全保護系のプロセス計装は、不正アクセス行為その他の電子計算機に使用目的に沿うべき動作をさせず、又は使用目的に反する動作をさせる行為による被害を防止する設計とする。</u></p>	<p>【計測制御系統施設】（基本設計方針）</p> <p>1.3 安全保護装置等</p> <p>1.3.1 安全保護装置</p> <p>(2) 安全保護装置の不正アクセス行為等の被害の防止</p> <p>②安全保護装置は、外部ネットワークと物理的分離及び機能的分離、外部ネットワークからの遠隔操作の防止、ソフトウェアの内部管理の強化によるウイルス等の侵入の防止、物理的及び電氣的アクセスの制限、システムの据付、更新、試験、保守等で、承認されていない者の操作及びウイルス等の侵入を防止すること等の措置を講じることで②不正アクセス行為その他の電子計算機に使用目的に沿うべき動作をさせず、又は使用目的に反する動作をさせる行為による被害を防止できる設計とするとともに安全保護装置の論理演算機能（作動（起動）回路）については、デジタル回路及びアナログ回路で構成する設計とする。</p> <p>安全保護装置が収納された盤の施錠等により、ハードウェアを直接接続させない措置を実施すること及び安全保護装置のソフトウェアは設計、製作、試験及び変更管理の各段階で検証と妥当性の確認を適切に行うことで不正アクセスを防止する。</p>	<p>設計及び工事の計画の②は、設置許可申請書（本文）の②を具体的に記載しており、整合している。</p>	